

OLL 85-3323

Office of Legislative Liaison
Routing Slip

TO:		ACTION	INFO
	1. D/OLL		X
	2. DD/OLL		X
	3. Admin Officer		
	4. Liaison		X
	5. Legislation	X	
	6. []		X
	7. []		
	8. []		
	9. []		
	10. []		

SUSPENSE

~~28 Oct 85~~
Date

Action Officer:

Remarks:

~~GJ / 28 Oct 85~~
Name/Date

Recpt #

LEGISLATIVE LIAISON

85-3323



EXECUTIVE OFFICE OF THE PRESIDENT

OFFICE OF MANAGEMENT AND BUDGET

WASHINGTON, D.C. 20503

October 25, 1985

LEGISLATIVE REFERRAL MEMORANDUM

TO: Legislative Liaison Officer

Department of Commerce - Joyce Smith (377-4264)
General Services Administration - Ted Ebert (566-1250)
Department of Agriculture - Eric Mondres (447-7095)
Central Intelligence Agency
Department of Health & Human Services - Frances White (245-7750)
Office of Personnel Management - Gale Dugan (632-6514)
National Security Council


**SUBJECT: National Security Agency proposed testimony on
H.R. 2889 -- Computer Security Act.**

The Office of Management and Budget requests the views of your agency on the above subject before advising on its relationship to the program of the President, in accordance with OMB Circular A-19.

A response to this request for your views is needed no later than

4:00 p.m. -- MONDAY -- OCTOBER 28, 1985

Questions should be referred to Constance J. Bowers (395-3457), the legislative analyst in this office.


James C. Murr for
Assistant Director for
Legislative Reference

Enclosures

cc: Ed Springer
Robert Dotson
Kevin Scheid
Sherry Alpert

STATEMENT OF DR. ROBERT L. BROTZMAN
DIRECTOR, NATIONAL COMPUTER SECURITY CENTER

BEFORE THE
SUBCOMMITTEE ON TRANSPORTATION, AVIATION
AND MATERIALS
AND THE
SUBCOMMITTEE ON SCIENCE, RESEARCH
AND TECHNOLOGY
COMMITTEE ON SCIENCE AND TECHNOLOGY

OCTOBER 30, 1985

Mr. Chairman and Members of the Subcommittees:

Thank you for this opportunity to testify on H.R. 2889, the Computer Security Research and Training Act of 1985, and to address the government's capacity for carrying out computer security research and training activities. I would like to discuss why the government's present computer security structure, supported by National Security Decision Directive 145 (NSDD 145), represents the best approach to providing computer security research and training and why, therefore, we do not support H.R. 2889; nor do we support the recently amended version of the bill reported out by the Legislation and National Security Subcommittee of the House Government Affairs Committee.

Raising computer security awareness across the entire government and providing the training needed for the managers, computer operations professionals, and computer users is an enormous undertaking. A general plan for providing this training has been prepared by the National Computer Security Center and initial contacts have been made with defense and civil agencies of the government encouraging their participation in the planning and execution of this training task.

One of the Center's highest priorities is the building of strong training and awareness programs. Other efforts well under way include research and development, and vulnerability detection and reporting. Accurate information on computer vulnerabilities is a necessary prerequisite to a properly formulated training program. An aggressive research and development effort bolsters training as it provides the solutions to what I have described in the past as the curse that comes with the blessings of automation.

Until the signing of NSDD 145, the Center's activities were aimed at ensuring the security of data being processed by DoD computers. However, the majority of our programs can be, and are being, geared to the needs of civil agencies and in some cases to the private sector. For example, I have no doubt that the Computer Security Vulnerability Reporting Program being developed by the Center for DoD systems would, with minor modification, serve the rest of the government equally well. We have created the structure through which vulnerabilities discovered within specific systems are reported to a central point. Some vulnerabilities are system-unique; but, whenever the weakness is found to be in an operating system, in a generalized software module, or in the hardware used in multiple systems, the vulnerability information and the best remedial action will be shared with all users of the faulty component. The benefits to be realized from a centralized program are obvious.

We will use the vulnerability data to plug holes. The information collected will also improve our knowledge of the weaknesses and strengths of computer systems, and that knowledge will be used to help guide and shape our training and awareness programs--programs that are now being geared to a government-wide audience.

The Center has developed a National Computer Security Education Plan. It was formed from the NSDD 145 direction that "technical security material, other technical assistance, and other related services of common concern," as required to accomplish the objectives of the Directive, are to be provided to "departments and agencies of the government and, where appropriate, to private institutions (including government contractors)."

We fully realize that the audience to be served is much too large to be served by the Center alone, or for that matter by any organization working alone. The immense size and diversity of functions performed in government suggest that it is not very useful to talk about national programs for education and awareness. Rather, we must think in terms of a national-level effort to ensure that each organization within the federal government has adequate computer security education and awareness programs. For large agencies, this may mean a full-fledged program with courses developed and conducted in-house. Smaller agencies may have only an awareness program and rely on other sources for formal courses. For example, some organizations, such as the Department of Energy, already have active, successful education and awareness programs established. However, other organizations, especially smaller ones, are looking to government training organizations to provide the formal courses and more tailored training sessions. The DoD Computer Institute, the Office of Personnel Management, and the Computer Security Center, all include computer security courses in their curricula. Computer security courses are also available at some academic institutions. They should not be overlooked as valuable sources of security education. And, of course, there are the courses available from the private sector: from firms that provide them for profit, and from non-profit organizations such as professional societies.

The educational services of the Center are directed toward four groups: the general user of computer systems; managers of computer systems; education specialists; and computer science people who require specialized training.

In general, our program is geared toward (1) developing state-of-the-art computer security education modules and making them available to those who need them, (2) assisting others in setting up programs, and (3) acting as a clearinghouse for available information.

I would like to outline some of our specific recent accomplishments in education and awareness.

We offer a National-level course for managers that provides a general introduction to the need for computer security and what can be or is being done to provide it.

We offer a course on advances in computer security R&D for personnel from throughout the government. This week-long course gives computer science professionals a firm basis for understanding how to implement security. We have held other technically oriented courses in artificial intelligence, verification tools, and software-oriented computer architecture.

We have developed the first five modules for what we call our "roadshow." This is a training session tailored to a specific organization. The roadshow is a multi-media approach to providing information on computer security to an organization at its site. With instructional modules, the roadshow can range from a 1-hour to a several-day presentation, covering topics such as the threat to information in computers, risk assessment, standards for evaluating security, and software and hardware available to improve security.

Our awareness activities include an industrial symposium, held last spring; awareness posters, which are distributed to a broad spectrum of government agencies; and two awareness video tapes (we have distributed nearly 600 copies of these since this June).

One activity that we hope will have strong impact on education and awareness is a symposium that we are sponsoring, and which is being held today, for computer security educators in the federal government. We are meeting to learn about each others' programs and to discuss how we can help each other, especially in sharing resources such as course materials. We intend to make this an annual event, and expect it to increase in attendance and length from this year's first effort.

In support of what we see as our role as an information clearinghouse, we are in the process of setting up several data bases on computer security education-related information. Listings from the data bases will be given broad distribution. The first data base is on educational activities. It will include courses, workshops, and seminars offered by government agencies, by academic institutions, and by the private sector. The data base is nationwide in scope.

In FY 86, we will continue the existing courses, develop ten more modules for our roadshow, produce three more video tapes, and publish a handbook describing how to set up an awareness program.

By next spring, we hope to have a data base on upcoming conventions and conferences, and one on computer security education and awareness products.

In all our education and awareness activities at the Center, we follow a philosophy of openness and sharing. All the education and training material that we develop is available to other organizations. We are trying to "package" our resources to ease this sharing. Often the information can be shared at little or no cost to the receiving agency. For example, to receive a copy of our video tapes, we ask only that we be sent a blank tape.

Through an academic outreach program, our education and training people have been assisting the academic community in getting computer security into computer science courses. A spring conference is planned for further discussions with academicians on this subject. We also will be encouraging the inclusion of computer security awareness in management courses. Educational institutions, both government and private, are recognizing that managers need to be "computer literate." We believe that being literate must include an appreciation of security requirements.

During FY 86, we will begin our own entry-level training program. This program will be a mix of courses, video's, reading, and discussion groups that together will teach our incoming Center personnel what they need to know about computer security. There are "tracks" for nine different kinds of employees--from clerical persons to managers to system evaluators. The modules that make up this program, like those in our roadshow, will be available to any requesting organization. We are packaging our modules so that they are complete and ready for use--scripts, graphics, exercises, video's--whatever is needed by a particular organization.

We have published, or in some cases are preparing for publication, computer product evaluation criteria, guidelines for applying certain levels of security in specific environments, and guidance on subjects such as audit, discretionary access control, office automation, data remanence, and database management. Many of these publications are adaptable to the civil sector.

Let me single out one of the several areas in which we have been dealing with civil sector elements of the government. This past August, letters were sent to the heads of 79 organizations in the Legislative and Executive Branches, independent government establishments, and government corporations, offering computer security assistance, outlining the services offered by the Center, and requesting a point of contact for computer security matters. A team has been formed to introduce these organizations to the Center's mission, discuss the need to protect sensitive data, and make them aware of the security measures available to protect this data.

The response has been extremely enthusiastic. I have the clear impression that the groups we contacted had concerns and

questions about computer security, and were relieved to find that someone was willing and able to supply answers. Last month alone the team visited 14 government organizations in the civil sector, all of whom were very receptive to what we had to say. These visits were made to the Department of Agriculture; Department of the Treasury; Office of Technology Assessment; Department of Labor; Department of Commerce; Farm Credit Administration; Department of Transportation; National Aeronautics and Space Administration; Department of Education; Veterans Administration; Department of the Interior; Department of Justice; Department of Health and Human Services; and the Office of Personnel Management. The list is growing, and the team will be busy for some time. It is obvious that the interest is out there, and we plan to do our best to provide the assistance that is being sought and that is drastically needed.

The R&D program is challenging. Our greatest challenge lies in converting research breakthroughs into marketable security products. The approach we have taken is to divide our efforts into five distinct areas: secure computer system architecture, secure data base management systems (DBMS's), aids to evaluation, modeling and verification, and network security. Each of these subprograms, which comprise the Consolidated Computer Security Program (CCSP), explores particular aspects of computer security R&D. Most of these subprograms are distinct from research areas pursued at NBS; however, in some areas, the work of the Center and NBS is complementary. Complementary R&D efforts by the Center and NBS are ongoing or planned in the areas of developing risk analysis methodology; evaluating limited-function security products; participating in network security methodology; and evaluating criteria development and network security protocols. The Center and NBS regularly seek each other's technical assistance in these matters.

Presently, a Technical Review Group (chaired by the Center's R&D office and consisting of representatives from the Army, Navy, Air Force, Defense Communications Agency, and Defense Intelligence Agency) manages and allocates funds for the five subprograms. We have invited NBS with their private sector experience in computer research and standards development to become a full member of the Group. Since the current membership is DoD-oriented, NBS could bring to this forum a civil agency perspective and could identify civil agency needs not covered in our program. Also, as the acknowledged expert on the concerns of the private sector, NBS membership could assure that full consideration will be given to private industry's concerns.

We believe that our Computer Security R&D program provides the solid framework needed to convert research breakthroughs into viable products. By maintaining our cooperative and complementary

relationship with NBS, we can better address the needs of the civil agencies and the private sector.

In virtually all of the activities I have mentioned we have relied on the support and cooperation of other government agencies, and we, in turn, freely support many of them, among the closest of which is NBS. We have had and will continue to have a close working arrangement that is highly beneficial to both parties. We have not yet encountered any subjects of disagreement concerning areas of responsibility. Functions that may seem to overlap we address together--very effectively I might add. Tasks clearly in the purview of one are often attacked with the help of the other.

Perhaps the best-known manifestation of this cooperation is the annual Computer Security Conference, which has been cosponsored by the Center and NBS for the past eight years. Early this month, 950 people from 100 defense, civil, and private organizations gathered to discuss problems and accomplishments, and to exchange ideas. This number is double that of 1983, and includes 55 representatives of 8 nations on 4 continents. We share with NBS the satisfaction that comes with seeing the long-ignored subject of computer security draw such rapidly growing interest.

We agree with the recommendations of the Subcommittee on Transportation, Aviation, and Materials of the Committee on Science and Technology that the Administration view computer security in the broadest possible terms; establish a central focus with wide agency participation; review policy and improve related federal programs; and increase the role of the federal government in influencing public sector awareness. The existing government structure under NSDD 145 clearly is responsive to these concerns.

The responsibilities with which NBS is currently tasked--responsibilities which, in my opinion they impressively fulfill, do not conflict but rather complement those assigned to the National Computer Security Center under NSDD 145. The active role taken by NBS in the NTISSC's Subcommittee on Automated Information Systems Security will ensure that those responsibilities continue and that any potential duplication of effort is quickly identified and avoided. I see absolutely no erosion of the NBS role in computer security resulting from the implementation of NSDD 145. Existing programs at the Center and at NBS are generating effective momentum under the current NSDD 145 structure. I would not want to lose this momentum. Programs to get the computer security job done are in place and a cooperative effort is underway to attack and solve the computer security problem facing the government and private sector.

To summarize, the government has the capacity to do the computer security education and computer vulnerability research that is needed. We plan to work closely with other government

departments, as we do in most of our endeavors, where we depend heavily on the cooperative efforts of highly capable organizations such as the National Bureau of Standards. The program is in place and the effort has begun. It is aimed at the goals of H.R. 2889 and it is easily adapted to the needs of the wide range of computer users we are trying to reach.

What all of us are trying to do is too important and time-critical to allow for delays and regrouping. I assure you that your concerns are my concerns. The technological disasters we are trying to avert are very real. We have to get on with the job, and with your committee as an ally, I am sure we can get the job done.